

Serial No.: 09/539,927

Attorney's Docket No.:10559/151001
Intel Corporation: P7976Amendment to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Currently Amended) A machine-implemented method, comprising:

obtaining policy rules, and simplifying said policy rules to form simplified policy rules, wherein a policy rule comprises one or more conditions and one or more values associated with the one or more conditions, the one or more conditions to be evaluated for network communications based on the one or more values, and said simplifying comprises eliminating at least one of any redundant conditions and values from the policy rule based at least in part on condition-type information of the one or more conditions; and

based on said simplified policy rules, creating an access control list adapted to configure a network device, including creating at least one array of included conditions and at least one array of excluded conditions from the policy rules; and

using the access control list to generate access filters that configure the network device to control network communications in the network device, including generating, after redundancy checks, one or more deny filters by combining the at least one array of excluded conditions and the at least one array of included conditions, and wherein generating the

Serial No.: 09/539,927

Attorney's Docket No.: 10559/151001
Intel Corporation: P7976

access filters comprises adding one or more filters adapted to control access of a device to a component other than the network device in a network connected to the network device.

2. (Previously Presented) The method of claim 1 further comprising expanding the policy rules into value groups that represent conditions occurring in the network device associated with the policy rules.

3. (Previously Presented) The method of claim 2 wherein said simplifying comprises excluding conditions that would otherwise be implied by policy rules.

4. (Original) The method of claim 3 further comprising resolving inconsistent conditions that result from expanding the policy rules and excluding the policy rule conditions.

5-7. (Cancelled)

8. (Currently Amended) The method of claim 1 & further comprising generating permit filters by combining the at least

Serial No.: 09/539,927

Attorney's Docket No.: 10559/151001
Intel Corporation: P7976

one of the arrays of the included conditions with the remaining arrays of included conditions.

9. (Currently Amended) A system comprising:
- a first device adapted to disseminate policy rules in a network; and
 - a second device adapted to receive the policy rules disseminated on the network by the first device and adapted to perform operations comprising:
 - simplifying said policy rules to form simplified policy rules, wherein a policy rule comprises one or more conditions and one or more values associated with the one or more conditions, the one or more conditions to be evaluated for network communications based on the one or more values, and said simplifying comprises eliminating at least one of any redundant conditions and values from the policy rule based at least in part on condition-type information of the one or more conditions;
 - based on said simplified policy rules, creating an access control list adapted to configure a network device, including creating at least one array of included conditions and at least one array of excluded conditions from the policy rules; and

Serial No.: 09/539,927

Attorney's Docket No.: 10559/151001
Intel Corporation: P7976

using the access control list to generate access filters that configure the network device to control network communications in the network device, including generating, after redundancy checks, one or more deny filters by combining the at least one array of excluded conditions and the at least one array of included conditions, and wherein generating the access filters comprises adding one or more filters adapted to control access of a device to a component other than the network device in a network connected to the network device.

10. (Original) The system of claim 9 wherein the second device further comprises a permit filter.

11. (Original) The system of claim 10 further comprising a plurality of data-storage devices adapted to permit access to the second device.

12. (Original) The system of claim 9 wherein the second device further comprises a deny filter.

Serial No.: 09/539,927

Attorney's Docket No.: 10559/151001
Intel Corporation: P7976

13. (Original) The system of claim 12 further comprising a plurality of data-storage devices adapted to deny access to the second device.

14. (Currently Amended) An article comprising a computer-readable medium which stores computer executable instructions for managing policy rules on a network, the instructions causing a computing machine to perform operations comprising:

simplifying policy rules to form simplified policy rules, wherein a policy rule comprises one or more conditions and one or more values associated with the one or more conditions, the one or more conditions to be evaluated for network communications based on the one or more values, and said simplifying comprises eliminating at least one of any redundant conditions and values from the policy rule based at least in part on condition-type information of the one or more conditions;

based on said simplified policy rules, creating an access control list adapted to configure a network device, including creating at least one array of included conditions and at least one array of excluded conditions from the policy rules; and

Serial No.: 09/539,927

Attorney's Docket No.: 10559/151001
Intel Corporation: P7976

using the access control list to generate access filters that configure the network device to control network communications in the network device, including generating, after redundancy checks, one or more deny filters by combining the at least one array of excluded conditions and the at least one array of included conditions, and wherein generating the access filters comprises adding one or more filters adapted to control access of a device to a component other than the network device in a network connected to the network device.

15. (Previously Presented) The article of claim 14 wherein the operations further comprise expanding the policy rules into value groups, wherein value groups represent conditions occurring in the network device associated with the policy rules.

16. (Previously Presented) The article of claim 15 wherein the simplifying further includes excluding conditions that would otherwise be implied by the policy rules.

17. (Previously Presented) The article of claim 16 wherein the simplifying further includes resolving inconsistent

Serial No.: 09/539,927

Attorney's Docket No.: 10559/151001
Intel Corporation: P7976

conditions that result from expanding the policy rules and excluding the policy rule conditions.

18. (Currently Amended) A network device, comprising:
- a configurable management process located on the network device having instructions to effect operations comprising:
- receiving policy rules in the network device;
 - translating the policy rules into simplified rules, wherein a policy rule comprises one or more conditions and one or more values associated with the one or more conditions, the one or more conditions to be evaluated for network communications based on the one or more values, and said translating comprises eliminating at least one of any redundant conditions and values from the policy rule based at least in part on condition-type information of the one or more conditions;
 - creating an access control list adapted to configure the network device from the simplified rules, including creating at least one array of included conditions and at least one array of excluded conditions from the policy rules; and
 - using the access control list to generate access filters that configure the network device to control network

Serial No.: 09/539,927

Attorney's Docket No.:10559/151001
Intel Corporation: P7976

communications in the network device, including generating, after redundancy checks, one or more deny filters by combining the at least one array of excluded conditions and the at least one array of included conditions, and wherein generating the access filters further comprises adding one or more filters adapted to control access of a device to a component other than the network device in a network connected to the network device.

19. (Original) The device of claim 18 further comprising a connection to an external network.

20. (Original) The device of claim 19 wherein the external network is a local area network.

21. (Original) The device of claim 19 wherein the external network is the Internet.

22-24. (Cancelled)